Trustwave®

Australian Data Security Compromises

Size Doesn't Matter (Really!)

Presented by:

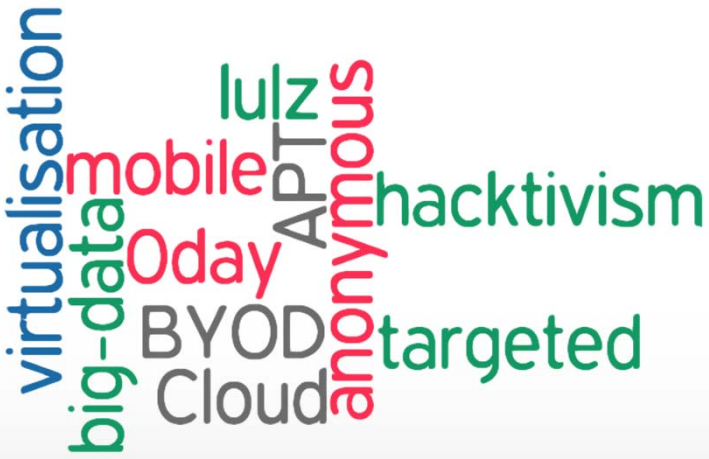
Marc Bown

Managing Consultant, SpiderLabs APAC

Trustwave SpiderLabs®

Trustwave SpiderLabs uses real-world and innovative security research to improve Trustwave products, and provides unmatched expertise and intelligence to customers.

Marketing made me do it



Trustwave SpiderLabs

3

Trustwave

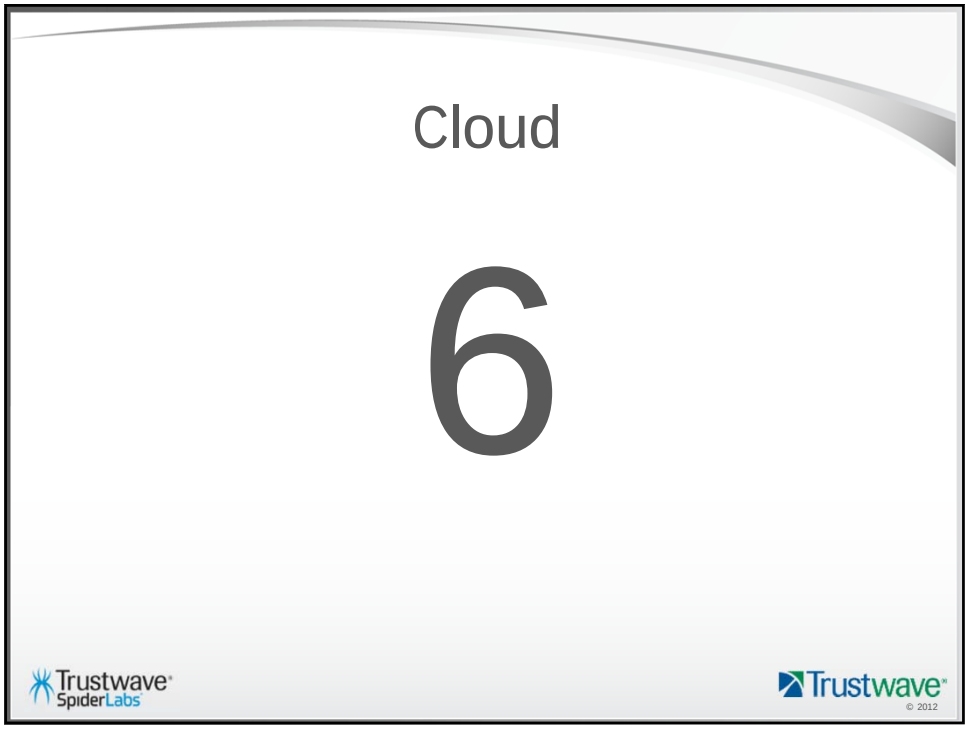
Buzzword Bingo

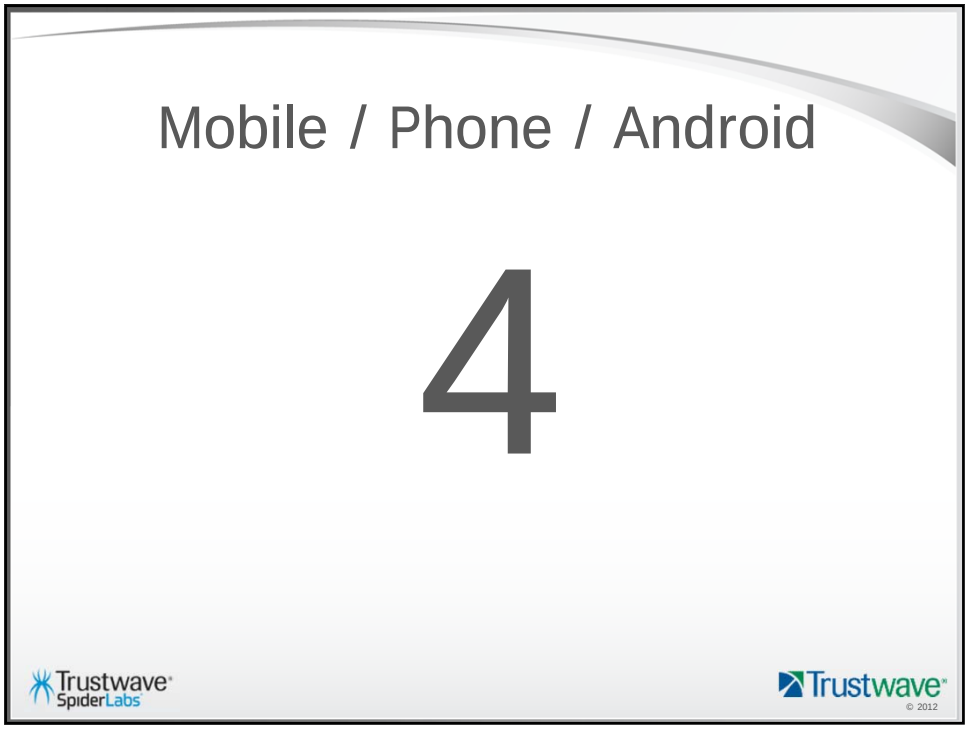
How many times are the following words mentioned in the conference agenda?

Trustwave SpiderLabs

4

Trustwave


Cloud
6
Trustwave SpiderLabs
Trustwave
© 2012


Mobile / Phone / Android
4
Trustwave SpiderLabs
Trustwave
© 2012

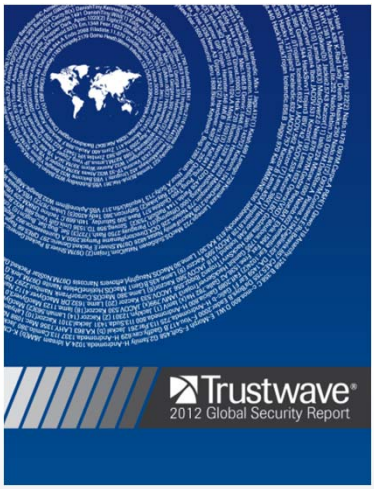
Targeted Attacks

2

Trustwave SpiderLabs

Trustwave

Trustwave 2012 Global Security Report



- Results from more than **300 incident response and forensic investigations** performed in **18 countries**.
  - More than 60 IR projects in Australia and New Zealand
- Analysis from more than **2,000 manual penetration tests** and **2 million network and application vulnerability scans**.
- Review of more than **25 different anti-virus vendors**.
- Usage and weakness trends of more **then 2 million real-world passwords** from corporate information systems.

Trustwave SpiderLabs

Trustwave

Targeted Attacks?

- Two reasons to perform an attack
  - Ideological
  - Financial gain
- Ideological = targeted attack
  - Attacker is motivated by their desire to raise awareness about a topic of interest relating to the target
  - Specific target may take longer to compromise but attacker invests time due to perceived ideological gain

Financial Gain

- Financial gain = path of least resistance
  - For many, this is a business
  - They wish to make the most the can by spending the least
  - Weakest link cliché applies
- Targets chosen on what they are, not who they are
  - Targets chosen as they have a specific vulnerability
  - Attackers invest in tooling targeting these vulnerabilities
  - These bring the marginal cost of compromise down to zero
  - Attackers job is to find as many targets as possible

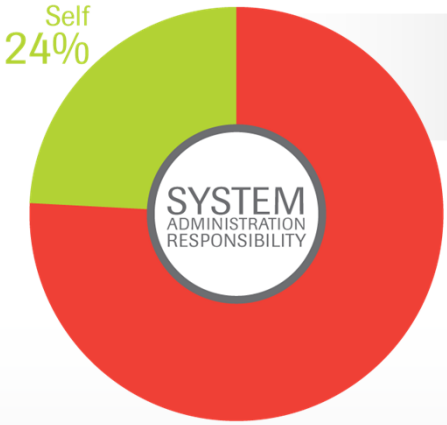
Targeted vs Opportunistic

- We investigated a single targeted case last year
- The rest were opportunistic attacks
- We as a community hear about targeted attacks
  - Compulsory disclosure in USA
  - Larger targets
  - Attackers release details (ideological)
- We don't hear about opportunistic attacks

"Why would they hack me..."

- This is the first thing we hear from a victim
  - "... I'm just a ..."
  - "... I only process a few credit cards a year"
- Almost all victim businesses were less than 50 employees
- "But my IT guy said everything was safe"

System Responsibility



75% of cases: a third party was responsible for a major component of system admin

Source: Trustwave 2012 Global Security Report

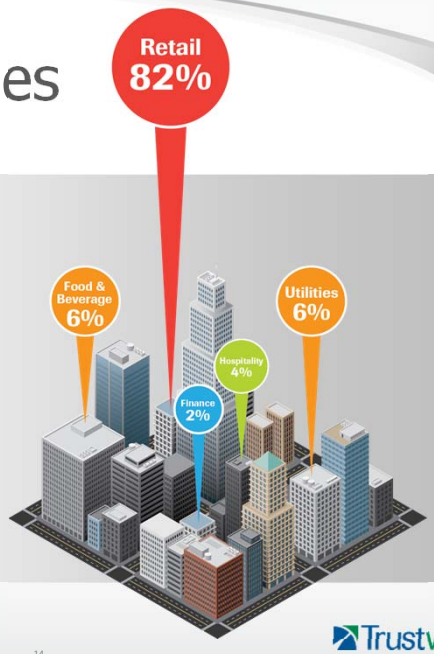
Trustwave SpiderLabs

13

Trustwave
© 2012

Victim Industries

- Those industries that we expect to be targets (e.g. Finance, critical infrastructure) tend to account for a small number of cases

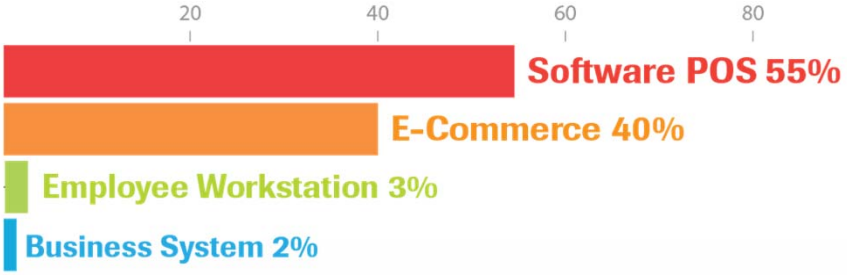


Trustwave SpiderLabs

14

Trustwave
© 2012

Victim Assets



Trustwave SpiderLabs

15

E-Commerce Attacks

Trustwave SpiderLabs

16

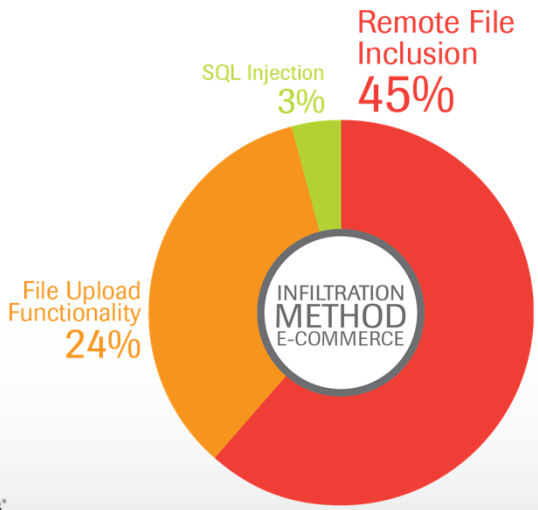
Average Victim

- Experienced bricks and mortar retail outlet that has expanded its presence online
- Majority are less than 5,000 transactions per year
- Most make use of off the shelf shopping cart applications
  - X-Cart, Lite Commerce, osCommerce, Zen Cart, Magento, Product Cart
- Use third parties for initial setup, hosting and maintenance
- Most sites are borderline profitable

Discovery

- Attackers locate potential victims a number of ways
  - Blindly scanning for vulnerabilities
    - Often focus on a single vulnerability
    - Sometimes scan for a handful
    - User agents indicate the use of industry standard tools (e.g. Havij for SQL Injection)
  - Googling for strings that identify certain web applications
    - E.g. Pages specific to osCommerce

Entry Method

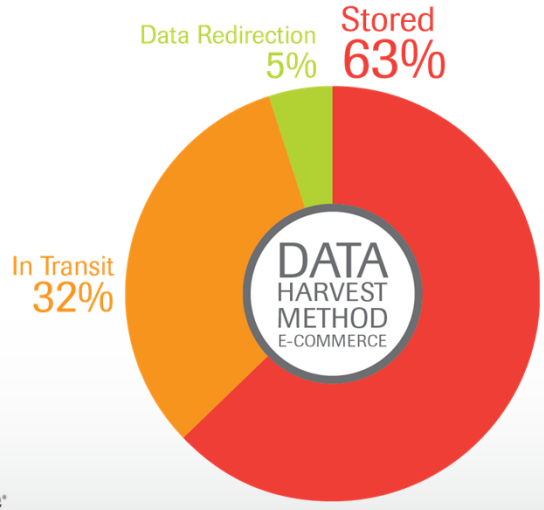


Trustwave SpiderLabs

19

Trustwave
© 2012

Data Harvest Method



Trustwave SpiderLabs

20

Trustwave
© 2012

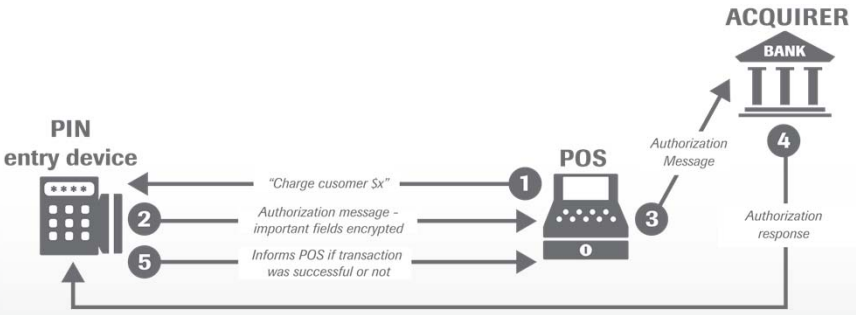
Point of Sale Attacks

Average Victim

- Experienced bricks and mortar retail outlet
- Often in a rural location
  - Most perceive some safety from not being in “the big smoke”
- Higher volume of transactions compared to e-commerce
- Most make use of one of a handful of software applications
- Use third parties for initial setup, hosting and maintenance

Discovery

- Unsure on how attackers discover potential victims
- May be as simple as port scanning Australian IP ranges
  - Some grouping of victims by location

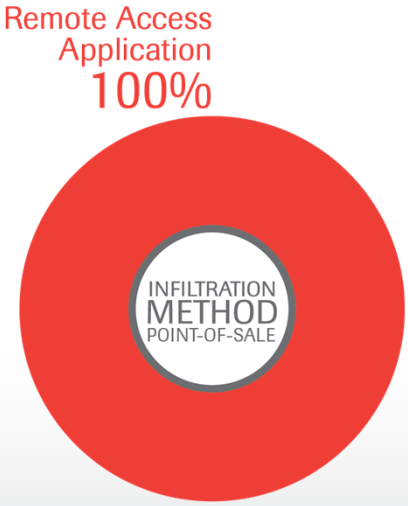


Trustwave SpiderLabs

23

Trustwave
© 2012

Entry Method

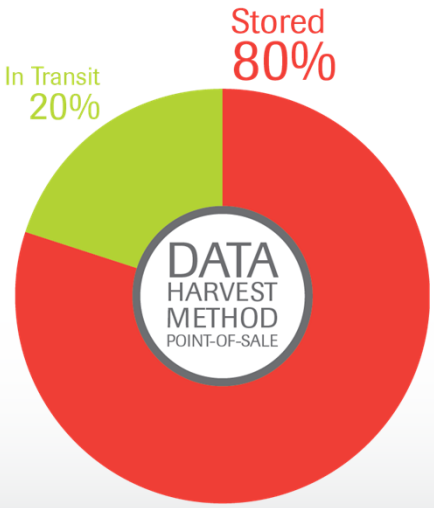


Trustwave SpiderLabs

24

Trustwave
© 2012

Data Harvest Method



Trustwave SpiderLabs

25

Trustwave

Malware Trends

Common and targeted

Trustwave SpiderLabs

Trustwave

Many Differences

Common

- **Self-propagation** through vulnerabilities or user actions
- **Widely distributed**
- Easily **detectable** by AV vendors

Targeted

- **No propagation** and may not exploits vulnerabilities
- Application/system specific
- Only **found in target environments**
- Most found in Trustwave 2011 investigations were **undetectable** by AV; *only 12% by top AV vendors*

Trustwave SpiderLabs

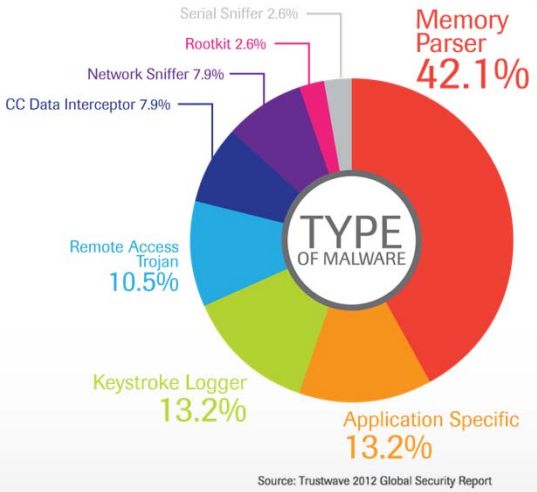
27

Trustwave

Targeted Malware Types

Popular Types

- **Memory Parser** obtains data in use out of system memory
- **Keystroke Loggers** target user and device input
- **Application Specific** hook the applications with access to target data



Source: Trustwave 2012 Global Security Report

Trustwave SpiderLabs

28

Trustwave

Our Defenses

Basic controls

Trustwave SpiderLabs

Trustwave

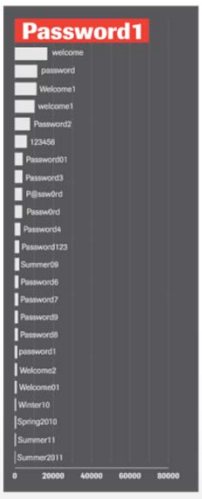
Passwords

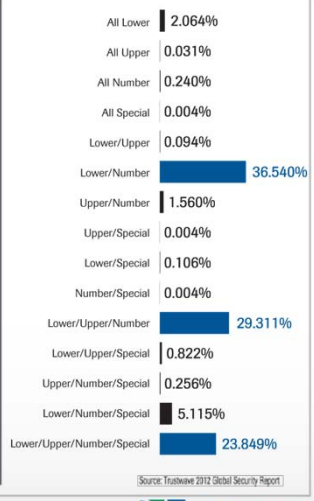
2.5+ Million Passwords Analyzed

- All in use within the enterprise

Common Weaknesses

- Shared 'admin' p/w
- New employee default p/w
- Poor complexity requirement
- 5% based on "password"
- 1% based on "welcome"

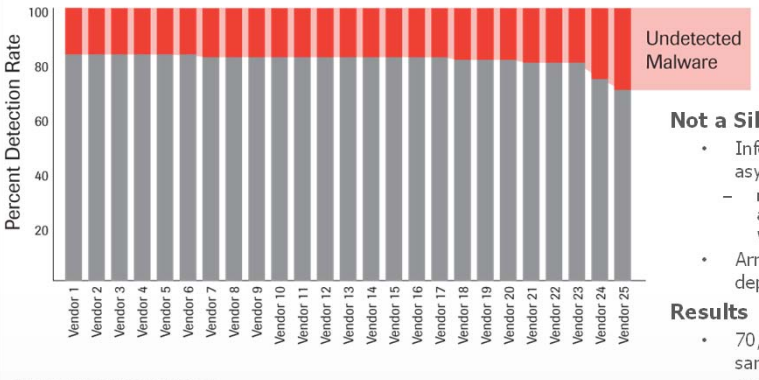




Trustwave SpiderLabs

Trustwave

Anti-Virus



Source: Trustwave 2012 Global Security Report

Not a Silver Bullet

- Information asymmetry
  - malware authors/signature writers
- Arms-race, signature dependence

Results

- 70,000 malicious samples
- A/V identified 81% of all samples
- Lowest vendor scored just 70%

Trustwave SpiderLabs

31

Trustwave

Summary

Trustwave SpiderLabs

32

Trustwave

Victims

- Mostly non-technical
- Often relying on a third party for IT
- Rarely a recognisable brand name
- All surprised to learn that they have been compromised

Attack Methods

- Attack methods were very simple
- Remote access with weak password for Point of Sales systems
- SQL Injection / File Upload / Remote File Inclusion for ecom
- All well understood easy to protect against issues
- No 0-days, no targeted e-mails or social engineering, no covering of tracks, nothing fancy

Defence

- Stopping the majority of the attacks is simple
- Focus on the basics
  - Password security
  - Secure remote access
  - Patch management
  - Data retention
  - Application security

Action Plan

- Highly targeted attacks are certainly a concern
- In planning for these, be careful not to lose sight of the basics
- Many of the basic controls are also helpful in preventing targeted attacks
- Ensure that your service providers are well behaved

Questions?

Trustwave SpiderLabs

Trustwave

Resources

Download the report: www.trustwave.com/GSR

Follow us online:

- Twitter: @Trustwave / @SpiderLabs
- Facebook: http://www.facebook.com/Trustwave
- LinkedIn: http://www.linkedin.com/company/trustwave
- Google+: https://plus.google.com/103260594120163717290

Trustwave SpiderLabs

Trustwave
© 2012